BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 2000113586
PUBLICATION DATE : 21-04-00

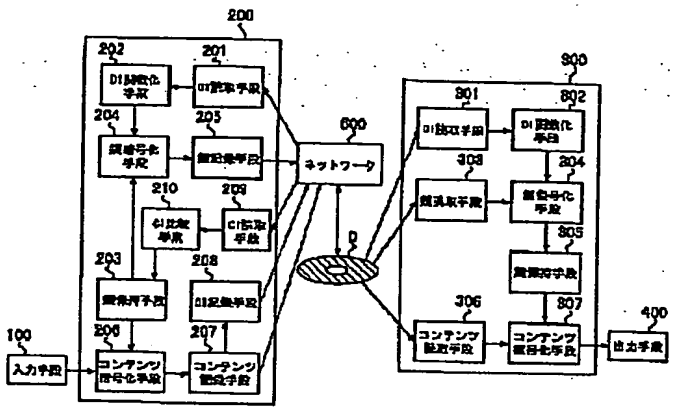
APPLICATION DATE : 01-10-98
APPLICATION NUMBER : 10280236

APPLICANT : VICTOR CO OF JAPAN LTD;

INVENTOR : HIRATA ATSUMI;

INT.CL. : G11B 20/10 H04L 9/10 H04L 9/32

TITLE : METHOD FOR PROTECTING INFORMATION AND INFORMATION RECORDING MEDIUM FOR PROTECTING INFORMATION



ABSTRACT : PROBLEM TO BE SOLVED: To prevent illicit copying and to easily permit copying to a person which legally obtains a right by recording the key encrypted by intrinsic information and the identification information respectively specific to respective pieces of the information, specifying the key encrypting the information by the identification information and reproducing the encrypted information by decryption.

SOLUTION: Input contents are encrypted by the key held in a key holding means 203 and are recorded on a disk D by a content recording means 207. The specific identification information is also recorded in the encrypted contents by a CI recording means 208. On the other hand, the intrinsic information of the disk D is read by a DI reading means 201 and is functioned by a DI functioning means 202 and the key of the key holding means 203 is encrypted and recorded on the disk D by a key encryption means 204. The key encrypting the contents is found out from the identification information by comparing the same with a content list and the key is encrypted by the intrinsic information of the copy disk and, therefore, the key may be decrypted from the intrinsic information of the copy disk by an information reproducing means 300.

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２０００－１１３５８６

（Ｐ２０００－１１３５８６Ａ）

(43)公開日　平成12年4月21日(2000.4.21)

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
G11B 20/10		G11B 20/10	H	5D044
H04L 9/10		H04L 9/00	621 A	5J104
9/32			673 E	
			673 C	

審査請求　未請求　請求項の数４　ＯＬ　（全１１頁）

(21)出願番号　特願平10-280236

(22)出願日　平成10年10月1日(1998.10.1)

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町3丁目12番地

(72)発明者　平田　渥美
神奈川県横浜市神奈川区守屋町3丁目12番地　日本ビクター株式会社内

(74)代理人　100083806
弁理士　三好　秀和　(外9名)

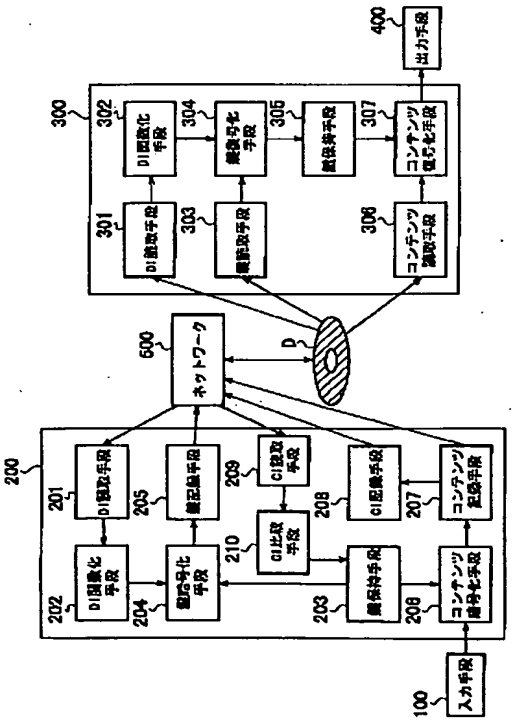
Ｆターム(参考)　5D044 AB05 AB07 CC04 DE49 GK17
5J104 AA13 AA16 EA17 NA02 NA30
PA14

(54)【発明の名称】情報保護方法及び情報を保護するための情報記録媒体

(57)【要約】

【課題】　情報を放送や通信手段を介して伝達し記録型ディスクに記録する際に、不正コピーを防止するとともに、正当に権利を得た者に対しては容易にコピーを許可することのできる情報保護方法を提供することにある。

【解決手段】　本発明の情報保護方法は、入力されたコンテンツを鍵によって暗号化して情報記録媒体Ｄに記録し、鍵によって復号化して再生する情報保護方法であって、各情報記録媒体に特有の固有情報と各コンテンツに特有の識別情報とを情報記録媒体Ｄに記録し、ＣＩ比較手段２１０において識別情報からコンテンツを暗号化した鍵を見つけることによってコンテンツを復号化して再生することを特徴とする。



1

【特許請求の範囲】

【請求項１】　それぞれ特有の固有情報を有する情報記録媒体に鍵によって情報を暗号化して記録し、前記情報記録媒体に記録された情報を前記鍵によって復号化して再生する情報保護方法であって、

前記固有情報によって暗号化された前記鍵と各情報にそれぞれ特有の識別情報とを前記情報記録媒体に記録し、前記情報を暗号化した前記鍵を前記識別情報によって特定し、前記暗号化された情報を復号化して再生することを特徴とする情報保護方法。

【請求項２】　それぞれ特有の固有情報を有する情報記録媒体に情報を暗号化して記録し、前記情報記録媒体に記録された情報を復号化して再生する情報保護方法であって、

前記固有情報によって暗号化された情報と関数化された前記固有情報とを前記情報記録媒体に記録し、前記関数化された固有情報を復号して得た固有情報から差分を生成することによって前記暗号化された情報を復号化して再生することを特徴とする情報保護方法。

【請求項３】　各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録され、さらに各情報毎にそれぞれ特有の識別情報が記録されていることを特徴とする情報を保護するための情報記録媒体。

【請求項４】　各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録され、さらに前記固有情報から生成された差分が記録されていることを特徴とする情報を保護するための情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、記録型ディスクに記録された情報を保護するための情報保護方法に関し、特に個々のディスクに特有の固有情報と個々のコンテンツに特有の識別情報とをディスクに記録することによって、不正コピーを防止するとともに、権利者に対しては容易にコピーを許可することのできる情報保護方法及び情報を保護するための情報記録媒体に関する。

【０００２】

【従来の技術】ＣＤ－Ｒ，ＰＤ，ＤＶＤ－ＲＡＭ，ＤＶＤ－ＲＷなどの記録型ディスク媒体（以下ディスクという）及び装置において、ネットワークあるいは放送を介して伝送され、正当に権利を得て１回記録することを許された場合、映画などの動画像、静止画像、音楽などのコンテンツは簡単に記録することができなければならない。また、記録後のディスクは、正規の装置であればどの装置を利用しても再生できるようにしたいという要求がある。

【０００３】一方、そのような記録型ディスク媒体及び装置において、不正にコピーされることを防止して著作

2

権を守る必要があるが、正当な権利で容易に記録・再生できることとコピーを防止することは背反しており両立させることが困難であった。

【０００４】そこで、このような矛盾を解決すべく従来の情報保護装置では、固有情報ＤＩを利用することによって不正なコピーを防止していた。

【０００５】図４に示すように、従来の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段１０と、一般的な情報記録媒体Ｄにコンテンツなどの情報を暗号化して記録する情報記録手段２０と、情報記録媒体Ｄに記録された情報を復号化して再生する情報再生手段３０と、復号化されたコンテンツなどの情報を出力する出力手段４０とを含んでいる。

【０００６】ここで、情報記録手段２０は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段２１と、このＤＩ読み取り手段２１によって読み取られた固有情報ＤＩを関数化あるいは暗号化（以下、関数化という）するＤＩ関数化手段２２と、このＤＩ関数化化手段２２によって関数化された固有情報Ｆ(ＤＩ)によって入力手段１０から入力されたコンテンツＣＴを暗号化するコンテンツ暗号化手段２３と、このコンテンツ暗号化手段２３によって暗号化されたコンテンツＥ(ＣＴ)を情報記録媒体Ｄに記録するコンテンツ記録手段２４とから構成されている。

【０００７】また情報再生手段３０は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段３１と、このＤＩ読み取り手段３１によって読み取られた固有情報ＤＩを関数化するＤＩ関数化手段３２と、情報記録媒体Ｄに記録された暗号化されたコンテンツＥ(ＣＴ)を読み取るコンテンツ読み取り手段３３と、このコンテンツ読み取り手段３３によって読み取られた暗号化されたコンテンツＥ(ＣＴ)を関数化された固有情報Ｆ(ＤＩ)によって復号化して出力手段４０へ出力するコンテンツ復号化手段３４とから構成されている。

【０００８】次に、この従来の情報保護装置の動作について説明する。

【０００９】まず、コンテンツＣＴが入力手段１０より入力されると、ディスクＤの固有情報ＤＩをＤＩ読み取り手段２１が読み取り、この固有情報ＤＩをＤＩ関数化手段２２で関数化してＦ(ＤＩ)とする。そして、コンテンツ暗号化手段２３において、入力されたコンテンツＣＴを関数化された固有情報Ｆ(ＤＩ)で暗号化してＥ(ＣＴ)とし、コンテンツ記録手段２４によってディスクＤに記録する。

【００１０】そして、ユーザーは情報再生手段３０においてディスクＤを再生する場合には、まずディスクＤからＤＩ読み取り手段３１によってディスクＤの固有情報ＤＩを読み取り、この固有情報ＤＩをＤＩ関数化手段３２で関数化してＦ(ＤＩ)とする。そして、次に暗号化されたコンテンツＥ(ＣＴ)をコンテンツ読み取り手段３３

によってディスクＤから読み取り、コンテンツ復号化手段３４において関数化された固有情報Ｆ（ＤＩ）によって復号化してコンテンツＣＴとし、出力手段４０に送り、出力することになる。

【００１１】また、図５に示す従来の情報保護装置では、図４の装置と同様に入力手段１０と、情報記録手段２０と、情報再生手段３０と、出力手段４０とを含んでいる。

【００１２】ここで、情報記録手段２０は、図４に示す装置の構成要素の他に、入力されるコンテンツＣＴを暗号化するための鍵ＫＥＹを保持する鍵保持手段２５と、この鍵保持手段２５により保持された鍵ＫＥＹを関数化された固有情報Ｆ（ＤＩ）によって暗号化する鍵暗号化手段２６と、この鍵暗号化手段２６によって暗号化された鍵Ｅ（ＫＥＹ）を情報記録媒体Ｄに記録する鍵記録手段２７とをさらに含んでいる。

【００１３】また情報再生手段３０は、図４に示す装置の構成要素の他に、情報記録媒体Ｄに記録された暗号化された鍵Ｅ（ＫＥＹ）を読み取る鍵読み取り手段３５と、暗号化された鍵Ｅ（ＫＥＹ）を関数化された固有情報Ｆ（ＤＩ）によって復号化する鍵復号化手段３６と、この鍵復号化手段３６によって復号化された鍵ＫＥＹを保持する鍵保持手段３７とをさらに含んでいる。

【００１４】次に、この従来の情報保護装置の動作について説明する。

【００１５】まず、コンテンツＣＴが入力手段１０より入力されると、コンテンツ暗号化手段２３において、入力されたコンテンツＣＴを鍵保持手段２５に保持された鍵ＫＥＹによって暗号化してＥ（ＣＴ）とし、コンテンツ記録手段２４によってディスクＤに記録する。一方、ＤＩ読み取り手段２１ではディスクＤの固有情報ＤＩを読み取り、この固有情報ＤＩをＤＩ関数化手段２２で関数化してＦ（ＤＩ）とする。そして、鍵暗号化手段２６において、鍵保持手段２５で保持された鍵ＫＥＹを暗号化してＥ（ＫＥＹ）とし、鍵記録手段２７によってディスクＤに記録する。

【００１６】そして、ユーザーは情報再生手段３０においてディスクＤを再生する場合には、まずディスクＤからＤＩ読み取り手段３１によってディスクＤの固有情報ＤＩを読み取り、この固有情報ＤＩをＤＩ関数化手段３２で関数化してＦ（ＤＩ）とする。そして、鍵読み取り手段３５によって読み取られた暗号化された鍵Ｅ（ＫＥＹ）を、鍵復号化手段３６において関数化された固有情報Ｆ（ＤＩ）で復号化して鍵ＫＥＹとし、鍵保持手段３７に保持する。

【００１７】一方、暗号化されたコンテンツＥ（ＣＴ）はコンテンツ読み取り手段３３によってディスクＤから読み取られ、コンテンツ復号化手段３４において鍵保持手段３７に保持された鍵ＫＥＹによって復号化してコンテンツＣＴとし、出力手段４０に送られ出力されることになる。

【００１８】また、図４と図５に示す従来の情報保護装置において、ネットワーク（放送型、ポイント・ツー・ポイント型、バスラインなど任意の形態を含む）を介してコンテンツを伝送する場合について、図６、図７にそれぞれ示す。基本的な構成は図４、図５と同じでディスクＤに記録する際にネットワーク５０が介在する。

【００１９】

【発明が解決しようとする課題】このように、上述した従来の情報保護装置では、確かに不正なコピーは防止できるものの、コンテンツを供給する側としては、不正なコピーを防止するということと同時に、正規の手続きをした者に対してはコピーを許し、それによって料金収入を得たいという要求があった。

【００２０】しかしながら、従来の情報保護装置では、たとえ正規に権利を得た者であっても、コピーされたディスクを再生することはできなかった。

【００２１】本発明は上記事情に鑑みてなされたものであり、その目的は、個々のディスクに特有の固有情報と個々のコンテンツに特有の識別情報とを情報記録媒体に記録することによって、不正コピーを防止するとともに、正当に権利を得た者に対しては容易にコピーを許可することのできる情報保護方法を提供することにある。

【００２２】

【課題を解決するための手段】上記目的を達成するために、第１の発明である情報保護方法は、それぞれ特有の固有情報を有する情報記録媒体に鍵によって情報を暗号化して記録し、前記情報記録媒体に記録された情報を前記鍵によって復号化して再生する情報保護方法であって、前記固有情報によって暗号化された前記鍵と各情報にそれぞれ特有の識別情報とを前記情報記録媒体に記録し、前記情報を暗号化した前記鍵を前記識別情報によって特定し、前記暗号化された情報を復号化して再生することを特徴とする。

【００２３】この第１の発明によれば、各情報記録媒体に特有の固有情報だけでなく、各情報に特有の識別情報とを利用することによって、不正コピーを防止できるとともに正規の手続きをした者は容易に情報記録媒体のコピーができるようになった。

【００２４】第２の発明である情報保護方法は、それぞれ特有の固有情報を有する情報記録媒体に情報を暗号化して記録し、前記情報記録媒体に記録された情報を復号化して再生する情報保護方法であって、前記固有情報によって暗号化された情報と関数化された前記固有情報とを前記情報記録媒体に記録し、前記関数化された固有情報を復号して得た固有情報から差分を生成することによって前記暗号化された情報を復号化して再生することを特徴とする。

【００２５】この第２の発明によれば、関数化された固有情報を復号化した得た固有情報から差分を生成し、こ

の差分を利用して暗号化された情報を復号化することによって、不正コピーを防止できるとともに正規の手続きをした者は容易に情報記録媒体のコピーができるようになった。

【００２６】第３の発明である情報を保護するための情報記録媒体は、各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録され、さらに各情報毎にそれぞれ特有の識別情報が記録されていることを特徴とする。

【００２７】この第３の発明によれば、各情報記録媒体に特有の固有情報だけでなく、各情報に特有の識別情報とを利用することによって、不正コピーを防止できるとともに正規の手続きをした者は容易に情報記録媒体のコピーができるようになった。

【００２８】第４の発明である情報を保護するための情報記録媒体は、各情報記録媒体毎にそれぞれ特有の固有情報が改変できない方法で、あるいは改変できないエリアに記録され、さらに前記固有情報から生成された差分が記録されていることを特徴とする。

【００２９】この第４の発明によれば、関数化された固有情報を復号化した得た固有情報から差分を生成し、この差分を利用して暗号化された情報を復号化することによって、不正コピーを防止できるとともに正規の手続きをした者は容易に情報記録媒体のコピーができるようになった。

【００３０】

【発明の実施の形態】以下、本発明に係る情報保護方法の第１の実施形態を図面に基づいて説明する。本実施形態の情報保護方法を実現する装置は、各情報記録媒体にそれぞれ特有の固有情報と各コンテンツに特有の識別情報とを利用することによって、コンテンツを暗号化するものである。

【００３１】図１は本実施形態の情報保護装置の構成を示すブロック図である。図１に示すように、本実施形態の情報保護装置は、動画像、静止画像、音楽などのコンテンツを入力する入力手段１００と、一般的な情報記録媒体Ｄにコンテンツなどの情報を暗号化して記録する情報記録手段２００と、情報記録媒体に記録された情報を復号化して再生する情報再生手段３００と、復号化されたコンテンツなどの情報を出力する出力手段４００とを含んでいる。

【００３２】ここで、情報記録手段２００は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段２０１と、このＤＩ読み取り手段２０１によって読み取られた固有情報ＤＩを関数化するＤＩ関数化手段２０２と、入力されるコンテンツＣＴを暗号化するための鍵ＫＥＹを保持する鍵保持手段２０３と、この鍵保持手段２０３により保持された鍵ＫＥＹを関数化された固有情報Ｆ（ＤＩ）によって暗号化する鍵暗号化手段２０４と、この鍵暗号化手段２０４によって暗号化された鍵Ｅ（ＫＥＹ）をネットワーク５００を介して情報記録媒体Ｄに記録する鍵記録手段２０５と、鍵保持手段２０３により保持された鍵ＫＥＹによって入力手段１００から入力されたコンテンツＣＴを暗号化するコンテンツ暗号化手段２０６と、このコンテンツ暗号化手段２０６によって暗号化されたコンテンツＥ（ＣＴ）をネットワーク５００を介して情報記録媒体Ｄに記録するコンテンツ記録手段２０７と、このコンテンツ記録手段２０７によって記録された暗号化されたコンテンツＥ（ＣＴ）に特有の識別情報ＣＩをネットワーク５００を介して情報記録媒体Ｄに記録するＣＩ記録手段２０８と、情報記録媒体Ｄに記録されている識別情報ＣＩを読み取るＣＩ読み取り手段２０９と、コンテンツとそのコンテンツを暗号化した鍵との対応について記録したコンテンツリストを有し、このコンテンツリストと識別情報ＣＩとを比較し、コンテンツに対応する鍵を見つけるＣＩ比較手段２１０とから構成されている。

【００３３】また情報再生手段３００は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段３０１と、このＤＩ読み取り手段３０１によって読み取られた固有情報ＤＩを関数化するＤＩ関数化手段３０２と、情報記録媒体Ｄに記録された暗号化された鍵Ｅ（ＫＥＹ）を読み取る鍵読み取り手段３０３と、暗号化された鍵Ｅ（ＫＥＹ）を関数化された固有情報Ｆ（ＤＩ）によって復号化する鍵復号化手段３０４と、この鍵復号化手段３０４によって復号化された鍵ＫＥＹを保持する鍵保持手段３０５と、コンテンツ記録手段２０７によって情報記録媒体Ｄに記録された暗号化されたコンテンツＥ（ＣＴ）を読み取るコンテンツ読み取り手段３０６と、暗号化されたコンテンツＥ（ＣＴ）を鍵保持手段３０５に保持された鍵ＫＥＹによって復号化して出力手段４００へ出力するコンテンツ復号化手段３０７とから構成されている。

【００３４】次に、本実施形態の情報保護装置の動作について説明する。

【００３５】まず、コンテンツＣＴが入力手段１００より入力されると、コンテンツ暗号化手段２０６において、入力されたコンテンツＣＴを鍵保持手段２０３に保持された鍵ＫＥＹによって暗号化してＥ（ＣＴ）とし、コンテンツ記録手段２０７によってネットワーク５００を介してディスクＤに記録する。そして、この暗号化されたコンテンツＥ（ＣＴ）に特有の識別情報ＣＩもＣＩ記録手段２０８によって記録する。

【００３６】一方、ＤＩ読み取り手段２０１ではディスクＤの固有情報ＤＩをネットワーク５００を介して読み取り、この固有情報ＤＩをＤＩ関数化手段２０２で関数化してＦ（ＤＩ）とする。そして、鍵暗号化手段２０４において、鍵保持手段２０３で保持されている鍵ＫＥＹを暗号化してE_{DI}（ＫＥＹ）とし、鍵記録手段２０５によってネットワーク５００を介してディスクＤに記録する。

【００３７】次に、ユーザーが情報再生手段３００において情報記録媒体Ｄを再生する場合について説明する。まず、情報記録手段２００で正規に記録されたオリジナルのディスクＤを再生する場合には、まずディスクＤからＤＩ読み取り手段３０１によってディスクＤの固有情報ＤＩを読み取り、この固有情報ＤＩをＤＩ関数化手段３０２で関数化してＦ(ＤＩ)とし、鍵読み取り手段３０３によって読み取られた暗号化された鍵E_{DI}(ＫＥＹ)を、鍵復号化手段３０４において関数化された固有情報Ｆ(ＤＩ)で復号化して鍵ＫＥＹとし、鍵保持手段３０５に保持する。そして、コンテンツ読み取り手段３０６で、暗号化されたコンテンツＥ(ＣＴ)をディスクＤから読み取り、コンテンツ復号化手段３０７において鍵保持手段３０５に保持されている鍵ＫＥＹによって復号化してコンテンツＣＴとし、出力手段４００に送られ出力されることになる。

【００３８】次に、コピーされたディスクＤ'を再生する場合について説明する。この場合にはＤＩ読み取り手段３０１によって読み取られた固有情報ＤＩ'がオリジナルディスクＤの固有情報ＤＩと異なるので、このままではディスクＤ'を再生することができない。そこで、情報記録手段２００のＤＩ読み取り手段２０１によって固有情報ＤＩ'を読み取り、この固有情報ＤＩ'をＤＩ関数化手段２０２で関数化してＦ(ＤＩ')とする。

【００３９】また、ＣＩ読み取り手段２０９ではネットワーク５００を介してディスクＤに記録されている識別情報ＣＩを読み取り、ＣＩ比較手段２１０において、この識別情報ＣＩとコンテンツリストとを比較し、対応するコンテンツの鍵ＫＥＹを見つけ、鍵保持手段２０３で保持する。そして、鍵暗号化手段２０４においてこの鍵ＫＥＹをＤＩ関数化手段２０２で関数化されたＦ(ＤＩ')によって暗号化し、$E_{DI'}$(ＫＥＹ)として鍵記録手段２０５でネットワーク５００を介してディスクＤ'に記録する。この際、ディスクＤ'にはオリジナルのディスクＤの固有情報ＤＩで暗号化された鍵E_{DI}(ＫＥＹ)が記録されているが、その上に新たに暗号化された鍵$E_{DI'}$(ＫＥＹ)を重ね書きするか、あるいは別の領域に追記してもよい。ただし、追記する場合には再生時に最新の鍵についての情報を確認してから再生することになる。また、この新たに暗号化された鍵$E_{DI'}$(ＫＥＹ)をディスクＤ'に記録する際にコンテンツを供給する側では料金を徴収すればよい。

【００４０】そして、情報再生手段３００では、ＤＩ読み取り手段３０１によってディスクＤ'の固有情報ＤＩ'を読み取り、ＤＩ関数化手段３０２で関数化してＦ(ＤＩ')とする。そして、鍵読み取り手段３０３によって、新しく暗号化された鍵$E_{DI'}$(ＫＥＹ)を、鍵復号化手段３０４において関数化された固有情報Ｆ(ＤＩ')で復号化して鍵ＫＥＹとして鍵保持手段３０５に保持する。新たな暗号化された鍵$E_{DI'}$(ＫＥＹ)はＦ(ＤＩ')によって暗号化されているので、オリジナルディスクＤの固有情報ＤＩではなく、コピーディスクＤ'の固有情報ＤＩ'で復号化することができる。

【００４１】そして、コンテンツ読み取り手段３０６では暗号化されたコンテンツＥ(ＣＴ)をディスクＤ'から読み取り、コンテンツ復号化手段３０７において鍵保持手段３０５に保持されている鍵ＫＥＹによって復号化してコンテンツＣＴとし、出力手段４００に送られ出力されることになる。

【００４２】尚、本実施形態ではＤＩ関数化手段２０２によって固有情報ＤＩを関数化し、この関数化された固有情報Ｆ(ＤＩ)によってコンテンツＣＴを暗号化しているが、固有情報ＤＩを関数化せずに直接固有情報ＤＩによってコンテンツＣＴを暗号化することもできる。この場合には情報再生手段３００においても固有情報ＤＩを関数化することなく、固有情報ＤＩによってコンテンツＣＴを復号化する。

【００４３】また、本実施形態では、ネットワーク５００を介して情報記録媒体Ｄへの記録、読み取りを実行しているが、ネットワーク５００を介さずに情報記録手段２００から情報記録媒体Ｄに直接記録等してもよい。

【００４４】このように、第１の実施形態の情報保護装置では、識別情報ＣＩからコンテンツを暗号化した鍵を、コンテンツリストと比較することによって見つけ出し、その鍵をコピーディスクＤ'の固有情報ＤＩ'によって暗号化するので、情報再生手段３００ではコピーディスクＤ'の固有情報ＤＩ'から鍵を復号化することができ、従ってコピーディスクＤ'を再生することができる。

【００４５】また、コンテンツを供給する側としては、新たに暗号化された鍵$E_{DI'}$(ＫＥＹ)をディスクＤ'に記録する際に、料金を徴収すればよいので、利益を確保することができるとともに、ディスクコピーによってコンテンツの使用を許可できるのでコンテンツの流通性をよくすることができる。

【００４６】次に、第２の実施形態の情報保護方法について説明する。

【００４７】図２は第２の実施形態の情報保護方法を実現する装置の構成を示すブロック図である。図２に示すように、本実施形態の情報保護装置は、第１の実施形態の情報保護装置と同様に、入力手段１００と、情報記録手段２００と、情報再生手段３００と、出力手段４００とを含んでおり、情報記録手段２００は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩをネットワーク５００を介して読み取る第１ＤＩ読み取り手段２５１と、この第１ＤＩ読み取り手段２５１によって読み取られた固有情報ＤＩを関数化する第１関数化手段２５２と、この第１関数化化手段２５２で関数化された固有情報Ｆ(ＤＩ)によって、入力手段１００から入力されたコンテンツＣＴを暗号化するコンテンツ暗号化手段２５３

と、このコンテンツ暗号化手段２５３によって暗号化されたコンテンツＥ(ＣＴ)をネットワーク５００を介して情報記録媒体Ｄに記録するコンテンツ記録手段２５４と、第１ＤＩ読み取り手段２５１によって読み取られた固有情報ＤＩを第１関数化手段２５２と異なる関数で関数化する第２関数化手段２５５と、この第２関数化化手段２５５によって関数化された固有情報Ｆ’(ＤＩ)をネットワーク５００を介して情報記録媒体Ｄに記録するＤＩ記録手段２５６と、情報記録媒体Ｄに記録されている関数化された固有情報Ｆ’(ＤＩ)をネットワーク５００を介して読み取る第２ＤＩ読み取り手段２５７と、この関数化された固有情報Ｆ’(ＤＩ)を、第２関数化手段２５５で関数化したときの逆関数F'^{-1}（暗号の復号化を含む）によって復号化するＤＩ復号化手段２５８と、第１関数化手段２５２で関数化された固有情報Ｆ(ＤＩ)、Ｆ(ＤＩ’)の差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)を生成する差分手段２５９と、この差分手段２５９によって生成された差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)をネットワーク５００を介して情報記録媒体Ｄに記録する差分記録手段２６０とから構成されている。

【００４８】また情報再生手段３００は、情報記録媒体Ｄ毎にそれぞれ記録された固有情報ＤＩを読み取るＤＩ読み取り手段３０１と、このＤＩ読み取り手段３０１によって読み取られた固有情報ＤＩを関数化するＤＩ関数化手段３０２と、情報記録媒体Ｄに記録された差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)を読み取る差分読み取り手段３０８と、この差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)と関数化された固有情報Ｆ(ＤＩ’)とを合成して関数化された固有情報Ｆ(ＤＩ)を生成する合成手段３０９と、情報記録媒体Ｄに記録された暗号化されたコンテンツＥ(ＣＴ)を読み取るコンテンツ読み取り手段３０６と、このコンテンツ読み取り手段３０６によって読み取られた暗号化されたコンテンツＥ(ＣＴ)を、合成手段３０９によって生成された関数化された固有情報Ｆ(ＤＩ)によって復号化して出力手段４００へ出力するコンテンツ復号化手段３０７とから構成されている。

【００４９】次に、第２の実施形態の情報保護装置の動作について説明する。

【００５０】まず、コンテンツＣＴが入力手段１００より入力されると、ディスクＤの固有情報ＤＩを第１ＤＩ読み取り手段２５１が読み取り、この固有情報ＤＩを第１関数化手段２５２で関数化してＦ(ＤＩ)とする。そして、コンテンツ暗号化手段２５３において、入力されたコンテンツＣＴを関数化された固有情報Ｆ(ＤＩ)で暗号化してＥ(ＣＴ)とし、コンテンツ記録手段２５４によってネットワーク５００を介してディスクＤに記録する。一方、第２関数化手段２５５では第１ＤＩ読み取り手段２５１で読み取られた固有情報ＤＩを第１関数化手段２５２とは異なる関数Ｆ’によって関数化してＦ’(ＤＩ)とし、ＤＩ記録手段２５６においてネットワーク５００を介してディスクＤに記録する。

【００５１】次に、ユーザーが情報再生手段３００において情報記録媒体Ｄを再生する場合について説明する。まず、情報記録手段２００で正規に記録されたオリジナルのディスクＤを再生する場合には、まずディスクＤからＤＩ読み取り手段３０１によってディスクＤの固有情報ＤＩを読み取り、この固有情報ＤＩをＤＩ関数化手段３０２で関数化してＦ(ＤＩ)とする。ここで、オリジナルのディスクＤを再生する場合には、差分読み取り手段３０８では差分を読み取る必要はなく、合成手段３０９でも合成することはない。そこで、コンテンツ復号化手段３０７ではコンテンツ読み取り手段３０６によって読み取られた暗号化されたコンテンツＥ(ＣＴ)を復号化してコンテンツＣＴとし、出力手段４００に送り、出力することになる。

【００５２】次に、コピーされたディスクＤ’を再生する場合について説明する。この場合には、ＤＩ読み取り手段３０１によって読み取られた固有情報ＤＩ’がディスクＤの固有情報ＤＩと異なるので、このままではディスクＤ’を再生することができない。そこで、情報記録手段２００の第２ＤＩ読み取り手段２５７によって関数化された固有情報Ｆ’(ＤＩ)を読み取り、ＤＩ復号化手段２５８で逆関数F'^{-1}をかけることによって固有情報ＤＩを得る。このように、Ｆ’(ＤＩ)をあらかじめオリジナルのディスクＤに記録しておき、逆関数F'^{-1}を保存しておくことによって、オリジナルのディスクＤの固有情報ＤＩを復号化して得ることができる。また、逆関数F'^{-1}をコンテンツを供給する側のみが知るようにしておくことによって、不正にコピーされることを防止することもできる。

【００５３】そして、このようにして得た固有情報ＤＩを第１関数化手段２５２によって関数化し、Ｆ(ＤＩ)を得る。また、第１ＤＩ読み取り手段２５１ではコピーディスクＤ’の固有情報ＤＩ’を読み取り、第１関数化手段２５２で関数化してＦ(ＤＩ’)を得る。

【００５４】ここで、差分手段２５９では、関数化された固有情報Ｆ(ＤＩ)、Ｆ(ＤＩ’)の差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)を生成し、差分記録手段２６０によってネットワーク５００を介してディスクＤ’に記録する。この際、ディスクＤ’のＦ’(ＤＩ)が記録されている部分に重ね書きをしても、別のエリアに記録してＦ’(ＤＩ)を残しておいてもよい。また、この差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)をディスクＤ’に記録する際にコンテンツを供給する側では料金を徴収すればよい。

【００５５】そして、情報再生手段３００では差分読み取り手段３０８によって差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)をディスクＤ’から読み取り、この差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)とＤＩ関数化手段３０２で関数化されたＦ(ＤＩ’)とを合成手段３０９で合成してＦ(ＤＩ)を得る。このＦ(ＤＩ)によってコンテンツ復号化手段３０７で

は、コンテンツ読み取り手段３０６で読み取られた暗号化されたコンテンツＥ(ＣＴ)を復号化してコンテンツＣＴとし、出力手段４００に送り、出力することになる。

【００５６】尚、本実施形態では、ネットワーク５００を介して情報記録媒体Ｄへの記録、読み取りを実行しているが、ネットワーク５００を介さずに情報記録手段２００から情報記録媒体Ｄに直接記録等してもよい。

【００５７】このように、第２の実施形態の情報保護装置によれば、あらかじめＦ’(ＤＩ)をオリジナルのディスクＤに記録しておき、逆関数F'^{-1}をＤＩ復号化手段２５８に保存しておくことによって、オリジナルのディスクＤの固有情報ＤＩを復号化して知ることができる。さらに、このオリジナルディスクＤの固有情報ＤＩとコピーディスクＤ’の固有情報ＤＩ’とから差分を生成してコピーディスクＤ’に記録することによって、情報再生手段３００では、この差分とコピーディスクＤ’の関数化された固有情報Ｆ(ＤＩ’)とを合成してＦ(ＤＩ)を得ることができるので、暗号化されたコンテンツを復号化することができる。

【００５８】また、コンテンツを供給する側としては、差分Ｆ(ＤＩ)－Ｆ(ＤＩ’)をディスクＤ’に記録する際に、料金を徴収すればよいので、利益を確保することができるとともに、ディスクコピーによってコンテンツの使用を許可できるのでコンテンツの流通性をよくすることができる。

【００５９】さらに、逆関数F'^{-1}をコンテンツを供給する側のみが知るようにしておくことによって、不正にコピーされることを防止することもできる。

【００６０】次に、情報記録媒体への固有情報の記録について説明する。

【００６１】本発明の情報保護方法において、まず不正コピーを防止するためには情報記録媒体に記録されている固有情報ＤＩが容易に改竄できない方法で記録されていなければならない。

【００６２】同心円状あるいはスパイラル状に情報を記録する任意の追記型あるいは書換型の一般的な情報記録媒体（以下、ディスク媒体と証する）は、図３に示すように、一般利用者は記録することができない領域、すなわちＢＣＡ（バースト・カッティング・エリア）３やリードインエリア２などとユーザーが記録できる領域、データエリア１などで構成されることが多い。このようなディスク媒体において、固有情報ＤＩ（番号・記号・文字・データなど任意の形態でよい）を特定のエリアに記録するか、あるいは例えばディスク媒体生産時に記録しておく方式を用いることによって、ディスク媒体それぞれを識別することが可能となる。

【００６３】ここで、固有情報ＤＩとは、各ディスク媒体をそれぞれ識別可能な唯一、あるいは他のディスク媒体の固有情報ＤＩとは容易に一致しない情報のことである。また、特定のエリアとは、例えば図３のＢＣＡ（バースト・カッティング・エリア）３，リードインエリア２，データエリア１などに記録することができるが、これらの場所に限らず任意の場所に記録することができるものである。

【００６４】このような固有情報ＤＩは、ユーザーが記録できない、あるいは記録されているものを改竄できない方法で記録することが必要であり、例えばディスク上に機械的な凹凸であらかじめ記録しておいたり、強いレーザー光のオンオフなどでディスクの微小領域の組成や破壊による反射率の変化で記録したり、あらかじめ機械的に記録されている信号の一部を破壊するなどの方法で記録することができる。

【００６５】

【発明の効果】以上説明したように、本発明の情報保護方法及び情報を保護するための報記録媒体によれば、第１の実施形態では各ディスクに特有の固有情報だけでなく、各コンテンツに特有の識別情報ＣＩとを利用することによって、不正コピーを防止できるとともに正規の手続きをした者は容易にディスクのコピーができるようになった。

【００６６】第２の実施形態では、別の関数で関数化した固有情報Ｆ’(ＤＩ)をオリジナルのディスクＤに記録しておき、逆関数F'^{-1}をＤＩ復号化手段２５８に保存しておくことによって、オリジナルのディスクＤの固有情報ＤＩを復号化して知ることができ、さらに差分を利用することによって、不正コピーを防止できるとともに正規の手続きをした者は容易にディスクのコピーができるようになった。

【００６７】また、コンテンツを供給する側としては、正規の手続きをした者から料金を徴収することによって、利益を確保することができることになった。

【図面の簡単な説明】

【図１】本発明に係る情報保護方法を実現する装置の第１の実施形態の構成を示すブロック図である。

【図２】本発明に係る情報保護方法を実現する装置の第２の実施形態の構成を示すブロック図である。

【図３】情報記録媒体であるディスクの構成を示す図である。

【図４】従来の情報保護装置の構成を示すブロック図である。

【図５】従来の情報保護装置の構成を示すブロック図である。

【図６】図４に示す従来の情報保護装置において、ネットワークを介する場合における構成を示すブロック図である。

【図７】図５に示す従来の情報保護装置において、ネットワークを介する場合における構成を示すブロック図である。

【符号の説明】

１　データエリア

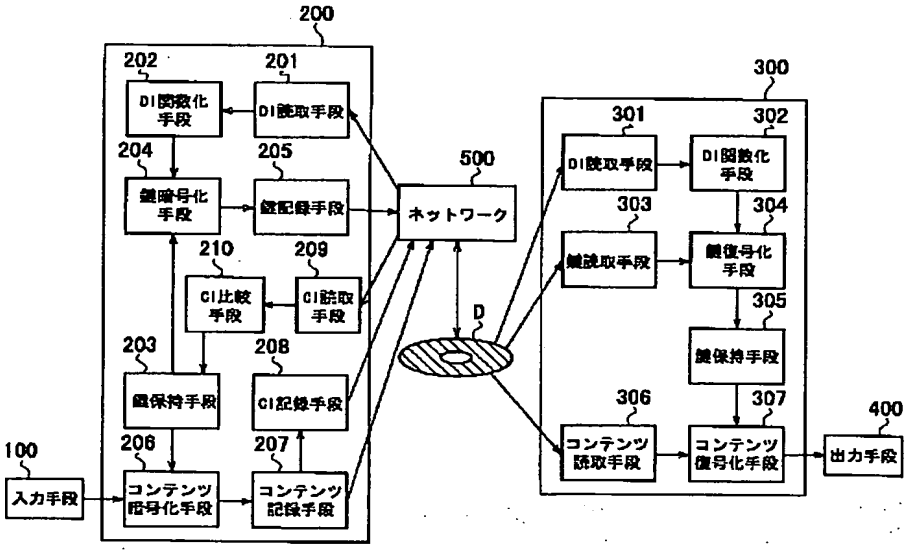
13

２　リードインエリア
３　バースト・カッティング・エリア
１０、１００　入力手段
２０、２００　情報記録手段
２１、３１　ＤＩ読み取り手段
２２、３２　ＤＩ関数化手段
２３　コンテンツ暗号化手段
２４　コンテンツ記録手段
２５　鍵保持手段
２６　鍵暗号化手段
２７　鍵記録手段
３０、３００　情報再生手段
３３　コンテンツ読み取り手段
３４　コンテンツ復号化手段
３５　鍵読み取り手段
３６　鍵復号化手段
３７　鍵保持手段
４０、４００　出力手段
５０、５００　ネットワーク
２０１、３０１　ＤＩ読み取り手段
２０２、３０２　ＤＩ関数化手段
２０３　鍵保持手段
２０４　鍵暗号化手段

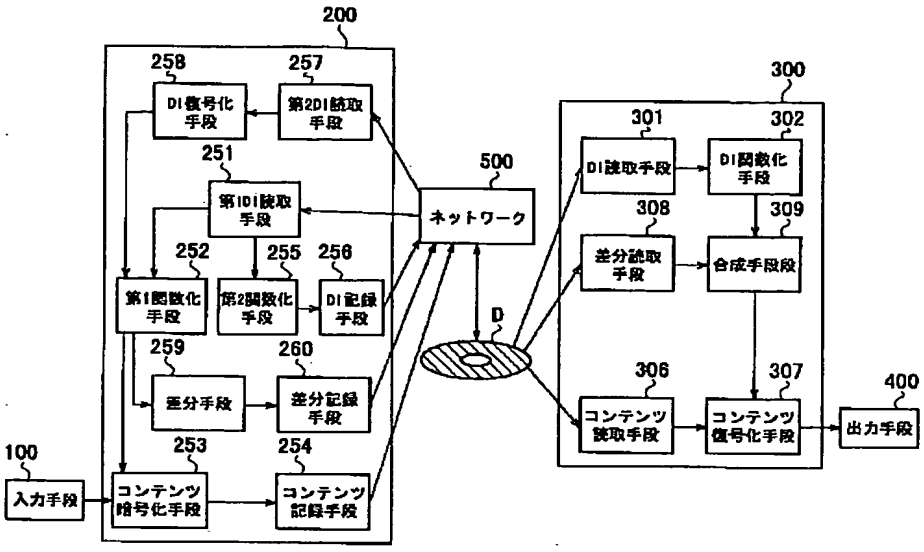
14

２０５　鍵記録手段
２０６、２５３　コンテンツ暗号化手段
２０７、２５４　コンテンツ記録手段
２０８　ＣＩ記録手段
２０９　ＣＩ読み取り手段
２１０　ＣＩ比較手段
２５１　第１ＤＩ読み取り手段
２５２　第１関数化手段
２５５　第２関数化手段
２５６　ＤＩ記録手段
２５７　第２ＤＩ読み取り手段
２５８　ＤＩ復号化手段
２５９　差分手段
２６０　差分記録手段
３０３　鍵読み取り手段
３０４　鍵復号化手段
３０５　鍵保持手段
３０６　コンテンツ読み取り手段
３０７　コンテンツ復号化手段
３０８　差分読み取り手段
３０９　合成手段
Ｄ　情報記録媒体

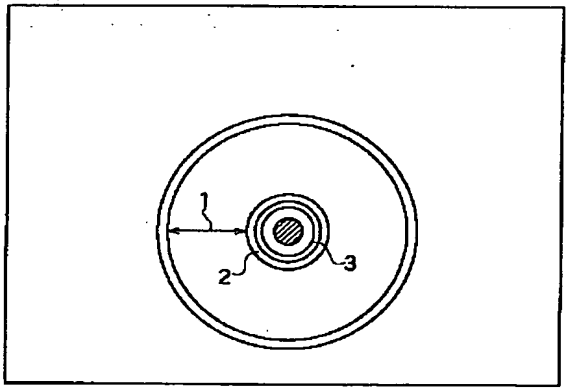
【図１】



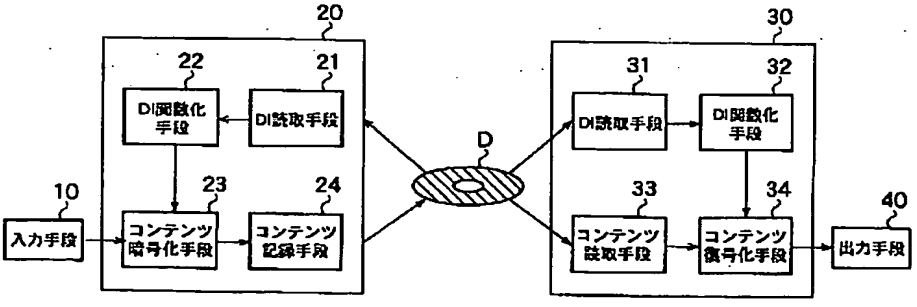
【図２】


200
258
DI復号化手段
257
第2DI読取手段
251
第1DI読取手段
252
第1関数化手段
255
第2関数化手段
256
DI記録手段
259
差分手段
260
差分記録手段
253
コンテンツ暗号化手段
254
コンテンツ記録手段
100
入力手段
500
ネットワーク
D
300
301
DI読取手段
302
DI関数化手段
308
差分読取手段
309
合成手段段
306
コンテンツ読取手段
307
コンテンツ復号化手段
400
出力手段

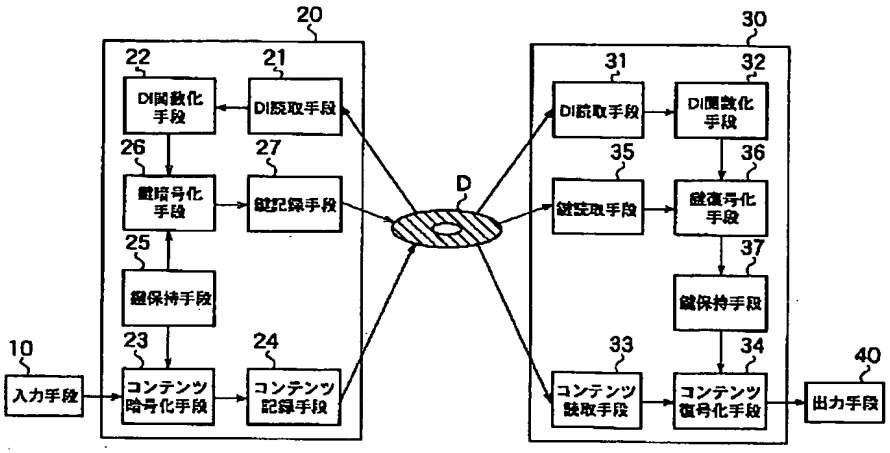
【図３】


1
2
3

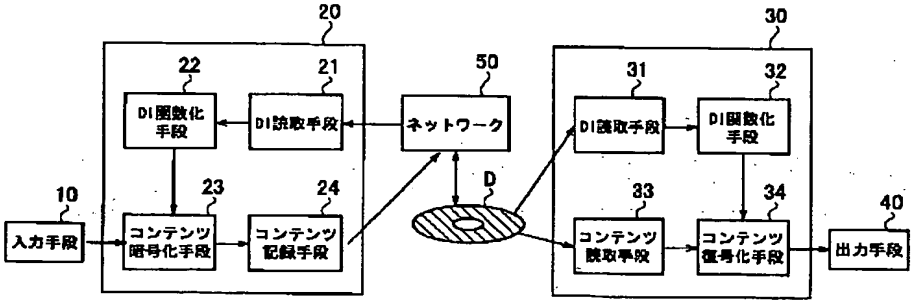
【図４】


20
22
DI関数化手段
21
DI読取手段
23
コンテンツ暗号化手段
24
コンテンツ記録手段
10
入力手段
D
30
31
DI読取手段
32
DI関数化手段
33
コンテンツ読取手段
34
コンテンツ復号化手段
40
出力手段

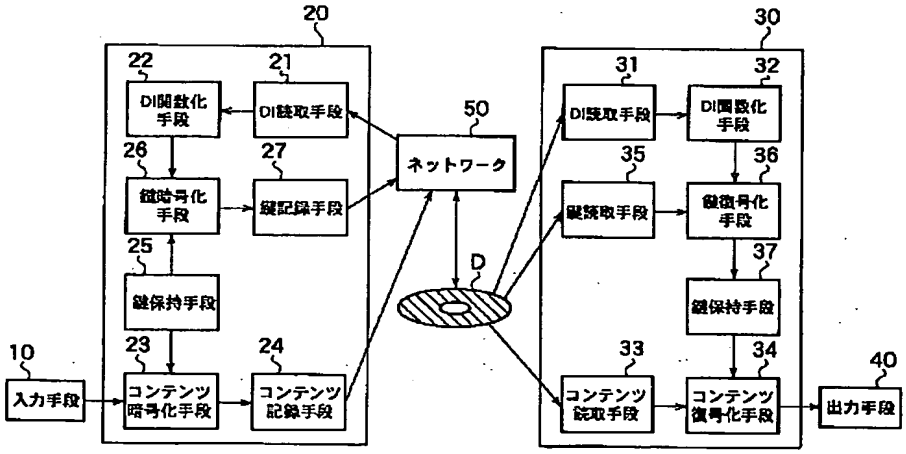
【図５】


20
30
22
21
31
32
DI圏数化手段
DI読取手段
DI読取手段
DI圏数化手段
26
27
35
36
鍵暗号化手段
鍵記録手段
D
鍵読取手段
鍵復号化手段
25
37
鍵保持手段
鍵保持手段
10
23
24
33
34
40
入力手段
コンテンツ暗号化手段
コンテンツ記録手段
コンテンツ読取手段
コンテンツ復号化手段
出力手段

【図６】


20
30
22
21
50
31
32
DI圏数化手段
DI読取手段
ネットワーク
DI読取手段
DI圏数化手段
D
10
23
24
33
34
40
入力手段
コンテンツ暗号化手段
コンテンツ記録手段
コンテンツ読取手段
コンテンツ復号化手段
出力手段

【図７】


20
30
22
21
31
32
DI圏数化手段
DI読取手段
50
DI読取手段
DI圏数化手段
ネットワーク
26
27
35
36
鍵暗号化手段
鍵記録手段
鍵読取手段
鍵復号化手段
D
25
37
鍵保持手段
鍵保持手段
10
23
24
33
34
40
入力手段
コンテンツ暗号化手段
コンテンツ記録手段
コンテンツ読取手段
コンテンツ復号化手段
出力手段

【手続補正書】
【提出日】平成１１年７月２７日（１９９９．７．２７）
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】図４
【補正方法】変更
【補正内容】
【図４】